JOSEPH W. COTCHETT (SBN 36324)
(jcotchett@cpmlegal.com)
MARK C. MOLUMPHY (SBN 168009)
(mmolumphy@cpmlegal.com)
ALEXANDRA P. SUMMER (SBN 266485)
(asummer@cpmlegal.com)
GWENDOLYN R. GIBLIN (SBN 181973)
(ggiblin@cpmlegal.com)
TORIANA S. HOLMES (SBN 282600)
(tholmes@cpmlegal.com)
COTCHETT, PITRE & McCARTHY, LLP
San Francisco Airport Office Center
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: (650) 697-6000
Facsimile: (650) 697-0577

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

MATTHEW BELDEN, Individually and on behalf of all other similarly situated California citizens, **Plaintiffs,** **v.** **EQUIFAX INC., a Georgia Corporation,** **Defendant.**	**Case No.** **CLASS ACTION COMPLAINT FOR:** **1. NEGLIGENCE;** **2. VIOLATION OF CALIFORNIA CIVIL CODE § 1798.80, *et seq.*;** **3. VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW; and** **4. UNJUST ENRICHMENT.** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

I. INTRODUCTION

1. This class action arises from one of the most pervasive data breaches in history. Preying on the lax online security barriers of Defendant **Equifax Inc.** ("Equifax"), hackers stole personal information from ***143 million*** Equifax user accounts, including the Equifax records of Plaintiff **Matthew Belden** ("Plaintiff").

2. Plaintiff brings this action individually and on behalf of a Class of ***California citizens*** whose personal information was stolen due to Equifax's failure to create and implement the proper security mechanisms to safeguard its customers' personal information. Approximately ***17 million*** California citizens' information has been compromised by Equifax.

3. Equifax, one of the three major consumer credit reporting agencies, was hacked and data of these consumers was stolen as a result of Equifax's conduct (the "Hack"). The Hack occurred during ***mid-May through July 2017*** and Equifax discovered the Hack on ***July 29, 2017***. However, Equifax waited more than a ***month*** from the end of the Hack — until ***September 7, 2017*** — to advise affected users that their private, personal information had been compromised. It was not until September 7, 2017 that Equifax disclosed ***for the first time*** that a website application vulnerability allowed hackers to breach past and current users' personal information, including names, ***Social Security numbers, birth dates, addresses, and in some instances driver's license numbers***. In addition, credit card numbers for approximately 209,000 U.S. users, and certain dispute documents with personal identifying information for approximately 182,000 U.S. users, were accessed. Equifax concealed the data breach, while at least three executive officers profited from selling thousands of shares of Equifax stock in the days following discovery of the breach.

4. The Hack is one of the largest ever and is the third major cybersecurity threat for Equifax since 2015. Despite a panoply of recent cyber-attacks and industry-wide warnings that Equifax must take active steps to improve its cyber security and data breach detection protocol, Equifax failed on multiple fronts to properly secure the personal information of its users. Equifax failed to create and implement proper security protocols to prevent and detect unauthorized breaches of its information security systems. Likewise, Equifax failed to

implement standard internet technology safeguards, amongst other failures.

5. As a direct result of Equifax's porous cybersecurity, Plaintiff, individually and on behalf of the Class of California citizens, has been damaged. This class action lawsuit follows.

II. JURISDICTION AND VENUE

6. This Court has jurisdiction under 28 U.S.C. § 1332(d) because: **(a)** this matter was brought as a class action under Fed. R. Civ. P. 23; **(b)** the class (as defined below) has more than 100 members; **(c)** the amount at issue exceeds $5,000,000, exclusive of interest and costs; and **(d)** at least one proposed Class member is a citizen of a state different from Equifax.

7. This Court has personal jurisdiction over Equifax because Equifax transacts substantial business in this judicial district.

8. Venue is proper in this Court under 28 U.S.C. § 1391 because, *inter alia*, Equifax regularly conducts substantial business in this district and is therefore subject to personal jurisdiction, and because a substantial part of the events giving rise to the Complaint arose in this district.

9. This action is not subject to arbitration. Equifax states on its website: "NO WAIVER OF RIGHTS FOR THIS CYBERSECURITY INCIDENT – In response to consumer inquiries, we have made it clear that the arbitration clause and class action waiver included in the Equifax and TrustedID Premier terms of use does not apply to this cybersecurity incident." (*See* https://www.equifaxsecurity2017.com/)

III. INTRADISTRICT ASSIGNMENT

10. Assignment to the San Francisco Division is appropriate under Local Civil Rule 3-2 because the actions that gave rise to the claims in this Complaint arose, in large part, in San Francisco County.

IV. PARTIES

11. Plaintiff Matthew Belden is a natural person, California citizen, and resident of Laguna Beach, California. Plaintiff Belden is one of the approximately 143 million Equifax users — including an estimated 17 million California citizens — whose personal information

was compromised because Equifax did not take reasonable steps to secure such information.

12. Defendant Equifax is a Georgia incorporated company headquartered at 1550 Peach Street, N.W., Atlanta, Georgia. Equifax is a member of the S&P 500®, and its common stock trades on the New York Stock Exchange under the symbol EFX.

V. FACTUAL BACKGROUND

A. EQUIFAX IS IN THE BUSINESS OF COLLECTING CONSUMERS' PRIVATE INFORMATION

13. Equifax's website reveals how problematic the Hack is when the Company's business is collecting users' private information: "Your credit history is a lot like a fingerprint: Everyone's credit history is unique, and no one's looks exactly the same." The credit reports Equifax produce are used by mortgage lenders, banks, credit card companies, retailers, and others who extend credit to users. Equifax is one of three major credit bureaus in the United States used for this purpose.

14. Equifax compiles all data about a particular consumer to provide a thorough credit report about the individual. Equifax can also provide data analysis so users or lenders can better understand a particular user's history.

B. EQUIFAX MAINTAINS A POROUS CYBERSECURITY INFRASTRUCTURE AND LAX INVESTIGATIVE REMEDIAL MEASURES

15. The hackers gained access to certain files in the company's system from mid-May to July and exploited a weak point in the website software.

16. To date, Equifax has provided only a vague description of how the Hack occurred, attributing it to "criminals" who "exploited a U.S. website application vulnerability." However, as additional information becomes available, it is increasingly apparent that Equifax is pointing fingers at "criminals" to deflect attention from its own reckless conduct that permitted the Hack. The Hack was possible due to a ***known*** vulnerability in Equifax's web server software.

17. Equifax uses Apache Struts software.[1] Apache Struts is a free, open-source MVC

[1] AnnaMaria Andriotis, Robert McMillan, and Christina Rexrode, "Equifax Comes Under Attach For Data Breach," *The Wall Street Journal* (Sept. 9-10) at B1-B2.

(model-view-controller) framework for creating Java web applications.[2] In early March 2017, security researchers publicly disclosed a bug in the Apache Struts software.

18. The vulnerability allowed remote users to access and gain significant control of web servers using the Apache Struts software. On or about March 9, 2017, the Apache Software Foundation issued Security Bulletin S2-045 titled “Possible Remote Code Execution when performing file upload based on Jakarta Multipart parser” (the “Security Bulletin”).

19. The Security Bulletin identified the vulnerability as “Critical” — the highest security rating. It indicated that the affected software included Struts versions 2.3.5 through 2.3.31 and versions 2.5 through 2.5.10. The fix for the problem was to “upgrade to Struts 2.3.32 or Struts 2.5.10.1.” Complete details on how to upgrade to those versions was readily available, free of charge, on the Apache Foundation Software Foundation website at https://struts.apache.org/docs/s2-045.html.

20. Rather than immediately taking steps to protect against the vulnerability, it appears that Equifax continued to operate without updating to the latest version of the Apache Struts software. Equifax’s decision not to immediately address the known and highly-publicized vulnerability irresponsibly left open a back door for hackers steal users’ confidential information.

21. Pamela Dixon, executive director of the World Privacy Forum, said of the breach, “This is about as bad as it gets. . . . If you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent.”

22. The hackers gained access to certain files in the company’s system from mid-May to July and exploited a weak point in the website software. In addition to the social security numbers and driver’s license numbers, other information compromised was names, date of birth and addresses. Credit card numbers for 209,000 consumers were stolen, while documents with personal information used in disputes for 182,000 people were also taken. Experts are saying the severity of the Equifax attack is potentially worse than any in history because the hackers were able to siphon more personal information — the keys that unlock consumers’ medical histories,

[2] Apache Struts website, https://struts.apache.org/

bank accounts and employee accounts.

23. Cybersecurity professionals have previously criticized Equifax for not improving its security practices. Last year, identity thieves successfully made off with critical W-2 tax and salary data from an Equifax website. And earlier this year, thieves again stole W-2 tax data from an Equifax subsidiary, TALX, which provides online payroll, tax and human resources services to some of the nation's largest corporations.

24. Equifax also houses much of the data that is supposed to be a backstop against security breaches. The company offers a service that provides companies with the questions and answers needed for their account recovery in the event customers lose access to their accounts. Patrick Harding, chief technology officer at Ping Identity, said, "If that information is breached, you've lost your backstop…"

25. Furthermore, Equifax's Privacy Policy affirmatively represents that it is "committed to protecting the security of [users'] information through procedures and technology designed for this purpose," and promises that "Before we provide [users] access to [their] credit file disclosure, we verify [their] identity." Personal information is information about users that is personally identifiable, even including users' name, address, email address, or phone number, and that is not otherwise publicly available.

26. Notwithstanding Equifax's lip service to cybersecurity and privacy, Equifax has in reality implemented ineffective cybersecurity measures and demonstrated a reticence to taking appropriate investigative and remedial action when the Hack was brought to its attention.

C. EQUIFAX'S OFFICERS DELAY DISCLOSING THE HACK IN ORDER TO TRADE STOCK BASED ON THEIR NON-PUBLIC KNOWLEDGE

27. In the days following discovery of the breach, and well before making any public disclosure, at least three Equifax executives profited by trading on the undisclosed information.

28. Equifax has stated that it discovered the Hack on July 29, 2017. Three days later, Equifax CFO John Gamble sold 6,500 shares, the President of Equifax's U.S. Information Solutions business unit sold 4,000 shares, and the President of another business unit Rodolpho Ploder sold 1,719 shares. The stock was sold for approximately $146 per share, reaping gross

proceeds of approximately $1,784,000 for these three executives.

VI. CLASS ACTION ALLEGATIONS

29. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2) and (b)(3), Plaintiff brings this action individually and on behalf of a class defined as follows: ***All California citizens whose personal information was compromised by the Hack disclosed by Equifax on September 7, 2017.***

30. Plaintiff is a member of the proposed Class of California citizens he seeks to represent.

31. This action is brought and may properly be maintained as a class action pursuant to 28 U.S.C. § 1332(d). This action satisfies the procedural requirements set forth in FED. R. CIV. P. 23.

32. Plaintiff's claims are typical of the claims of the Class Members. Plaintiff and all Class Members were damaged by the same wrongful practices of Defendant.

33. Plaintiff will fairly and adequately protect and represent the interests of the Class of California citizens. The interests of Plaintiff are coincident with, and not antagonistic to, those of the Class of California citizens.

34. Plaintiff has retained counsel competent and experienced in complex class action litigation.

35. Members of the Class of California citizens are so numerous that joinder is impracticable. Plaintiff believes that there are millions of California citizens in the Class.

36. Questions of law and fact common to the members of the Class predominate over questions that may affect only individual Class Members, because Defendant has acted on grounds generally applicable to the entire Class. Thus, determining damages with respect to the Class of California citizens as a whole is appropriate.

37. There are substantial questions of law and fact common to the Class consisting of California citizens. The questions include, but are not limited to, the following:

a. Whether Defendant failed to employ reasonable and industry-standard measures to secure and safeguard its users' personal information;

b. Whether Defendant properly implemented and maintained security measures to protect its users' personal information;

c. Whether Defendant's cybersecurity failures harmed the personal information of California citizens whose information was accessed by criminals or third parties who sought to gain financially from its improper use;

d. Whether Defendant negligently failed to properly secure and protect the personal information of California citizens;

e. Whether Plaintiff and other members of the Class of California citizens are entitled to injunctive relief; and

f. Whether Plaintiff and other members of the Class of California citizens are entitled to damages and the measure of such damages.

38. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated individuals to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. Plaintiff knows of no special difficulty maintaining this action that would preclude its maintenance as a class action on behalf of California citizens.

COUNT ONE

NEGLIGENCE

(Plaintiff individually and All Class Members)

39. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

40. Equifax had an affirmative duty to exercise reasonable care in safeguarding and protecting the personal information of its users. By maintaining their personal information in a database that was accessible through the Internet, Equifax owed Plaintiff and Class Members a duty of care to employ reasonable Internet security measures to protect this information.

41. Equifax, with reckless disregard for the safety and security of users' personal information it was entrusted with, breached the duty of care owed to Plaintiff and the Class by

failing to implement reasonable security measures to protect its users' sensitive personal information. In failing to employ these basic and well-known Internet security measures, Equifax departed from the reasonable standard of care and violated its duty to protect the personal information of Plaintiff and all Class Members. Equifax further breached its duty of care by allowing the breach to continue undetected and unimpeded for a period of time after the hackers first gained access to Defendant's systems.

42. The unauthorized access to the personal information of Plaintiff and all Class Members was reasonably foreseeable to Equifax.

43. Neither Plaintiff nor other Class Members contributed to the security breach or Equifax's employment of insufficient and below-industry security measures to safeguard personal information.

44. It was foreseeable that Equifax's failure to exercise reasonable care in protecting personal information of its users would result in Plaintiff and the other Class Members suffering damages related to the loss of their personal information.

45. As a direct and proximate result of Equifax's reckless conduct, Plaintiff and Class Members were damaged. Plaintiff and Class members suffered injury through the public disclosure of their personal information, the unauthorized access to accounts containing additional personal information, and through the heightened risk of unauthorized persons stealing additional personal information. Plaintiff and Class Members have also incurred the cost of taking measures to identify and safeguard accounts put at risk by disclosure of the personal information stolen from Equifax.

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

COUNT TWO

VIOLATION OF CALIFORNIA CIVIL CODE § 1798.80, *ET SEQ.*

(Plaintiff individually and All Class Members)

46. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

47. California Civil Code § 1798.80 *et seq*. (the "Customer Records Act") requires

any person conducting business in California and owning computerized data to disclose data breaches to affected users if the breach exposed unencrypted personal information.

48. The Customer Records Act also requires that the notice be made in the most expedient time possible without any unreasonable delay.

49. Equifax failed to notify users of the Hack in an expedient fashion.

50. The Hack qualifies as a "breach of security system" of Equifax within the meaning of Civil Code § 1798.82(g).

51. Equifax is liable to Plaintiff and the Class Members for $500.00 pursuant to Civil Code § 1798.84(c), or up to $3,000.00 per class member if Equifax's actions are deemed willful, intentional, and/or reckless.

52. Equifax is also liable for Plaintiff's reasonable attorneys' fees and costs pursuant to Civil Code § 1798.84(g).

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

COUNT THREE

VIOLATION OF CALIFORNIA BUSINESS AND PROFESSIONS CODE § 17200, *ET SEQ.*

(Plaintiff individually and All Class Members)

53. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

54. California's Unfair Competition Law ("UCL") is designed to protect consumers from illegal, fraudulent, and unfair business practices.

55. Equifax's practice of representing that it adequately protected users' financial and personal information, while Equifax in fact employed lax and ineffective security measures in order to cut costs, is a deceptive business practice within the meaning of the UCL. In fact, Equifax continues to employ lax and ineffective security measures as to the non-public, financial and personal information of users. Thus, Equifax continues to engage in deceptive business practices.

56. Equifax's practice of withholding information about the Hack from its users is

also a deceptive business practice within the meaning of the UCL, because users reasonably expect to be notified if their non-public, financial and personal information is compromised.

57. Equifax's practices are unfair because they allowed Equifax to profit while simultaneously exposing Equifax users, such as Plaintiff, to harm in the form of an increased risk of having their personal information stolen, which in fact occurred: the Hack. Such harm was not foreseeable to Equifax's users, who expected Equifax to employ industry-standard security measures, including cybersecurity firewalls to prevent a hack and investigative tools to timely discover one, and to promptly disclose any data breach.

58. Equifax's deceptive business practices induced Plaintiff and the Class to use Equifax's services and provide personal information to Equifax.

59. As a direct result of Equifax's deceptive business practices, Plaintiff and the Class have been and are being damaged.

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

COUNT FOUR

UNJUST ENRICHMENT

(Plaintiff individually and All Class Members)

60. Plaintiff incorporates by reference each of the preceding paragraphs as if fully set forth herein.

61. As a result of Equifax's misleading representations and omissions concerning the adequacy of its data security practices, Plaintiff and Class Members were induced to provide Equifax with their non-public, financial and personal information.

62. Equifax derived substantial revenues due to Plaintiff and the Class Members using Equifax's services, which maintained their non-public, financial and personal information, including through the sale of advertising directed at Plaintiff and the Class Members.

63. In addition, Equifax saved on the substantial cost of providing adequate data security to Plaintiff and the Class. Equifax's cost savings came at the direct expense of the privacy and confidentiality of the non-public, financial and personal information belonging to Plaintiff and the Class Members.

64. Plaintiff and the Class have been damaged and continue to be damaged by Equifax's actions, and Equifax has been unjustly enriched thereby.

65. Plaintiff and the Class are therefore entitled to damages as a result of Equifax's unjust enrichment, including the disgorgement of all revenue received and costs saved by Equifax as a result of the Hack.

WHEREFORE, Plaintiff and the Class pray for relief as set forth below.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class of California citizens, respectfully requests that the Court:

A. Determine that this action may be maintained as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3);

B. Direct that reasonable notice of this action, as provided by Federal Rule of Civil Procedure 23(c)(2), be given to the Class;

C. Appoint Plaintiff as Class Representative;

D. Appoint Plaintiff's counsel as Class Counsel;

E. Enter judgment against Defendant and in favor of Plaintiff and the Class;

F. Adjudge and decree that the acts alleged herein by Plaintiff and the Class against Defendant constitute negligence, violation of California Civil Code § 1798.80, *et seq.*, violation of California's Unfair Competition Law, and unjust enrichment;

G. Award all compensatory and statutory damages to Plaintiff and the Class in an amount to be determined at trial;

H. Award restitution, including the disgorgement of all revenue received and costs saved by Equifax as a result of the Hack, payable to Plaintiff and the Class;

I. Award punitive damages, including treble and/or exemplary damages, in an appropriate amount;

J. Enter an injunction permanently barring continuation of the conduct complained of herein, and mandating that Defendant and any successors in interest, be required to adopt and implement appropriate systems, controls, policies and procedures to protect the non-public, financial and personal information of Plaintiff and the Class;

K. Award Plaintiff and the Class the costs incurred in this action together with reasonable attorneys' fees and expenses, including any necessary expert fees as well as pre-judgment and post-judgment interest; and

L. Grant such other and further relief as is necessary to correct for the effects of Defendant's unlawful conduct and as the Court deems just and proper.

Dated: September 11, 2017 **COTCHETT, PITRE & McCARTHY, LLP**

*/s/ Mark C. Molumphy*__________________
MARK C. MOLUMPHY
Attorneys for Plaintiffs

JURY DEMAND

Plaintiff respectfully demands trial by jury on all issues so triable.

Dated: September 11, 2017 **COTCHETT, PITRE & McCARTHY, LLP**

*/s/ Mark C. Molumphy*__________________
MARK C. MOLUMPHY
Attorneys for Plaintiffs